guardtime

GDPR Compliance using KSI® Blockchain

Guardtime Whitepaper on VOLTA - its KSI® blockchain-based solution for GDPR.

David Shorthouse
GDPR Product Manager

Abstract

In April 2016, the EU Parliament and Council agreed upon the General Data Protection Regulations (GDPR), to go into effect on May 25, 2018. These regulations introduce tough new legal requirements and fines for companies relating to privacy and data protection of the personal data owned by EU individuals.

GDPR requires companies that handle the personal data of EU citizens to undertake major operational reform so that they can demonstrate data privacy and protection by both design and default.

This whitepaper explores GDPR and related data regulations, and introduces VOLTA; an application developed by Guardtime to provide an intelligent response to the new GDPR requirements. Guardtime believes that VOLTA is one of the first products to be developed for GDPR that utilises blockchain technology.

Keywords: *blockchain, KSI, GDPR, Volta*

"Guardtime's VOLTA product presents a path to GDPR certification that really stands out in today's marketplace"
Michael J Morrissey,
President & CEO International Insurance Society

The New Data Economy

The European Commission (EU) believes that the world is undergoing an exponential data explosion; that data itself has become a key new type of economic asset, a driver of growth and change, worthy of the most careful regulation and governance to ensure the future prosperity of the economic region.

> **"Those that know how to use [data] have a decisive competitive advantage in this interconnected world, through raising performance, offering more user-centric products and services, fostering innovation – often leaving decades-old competitors behind."**
> European Political Strategy Centre (EPSC)

At Guardtime[1] we wholeheartedly agree with this sentiment. However, holding pools of stand-alone data, without associated properties of **trust, integrity and provenance** is largely worthless. Without these properties, data held by a company quickly becomes hard to manage efficiently, impeding company performance and more worryingly leading to data inconsistency, with opportunities for data tampering and manipulation to go completely undetected.

Back in 2007, Guardtime was founded in response to the new data economy, to create tools to manage data efficiently at the most fundamental level. Its underlying KSI® blockchain technology has been in production since 2009, providing an industrial-scale information assurance backbone used today by governments, military institutions, and major enterprises.

Guardtime is responding to the continued evolution of the digital economy by developing applications that leverage its KSI blockchain technology to implement innovative data solutions.

Digital information is unlike any previous resource; it is extracted, refined, valued, bought and sold in different ways. It changes the rules for markets and it demands new approaches from regulators.

The quality of data has changed, too. There are no longer traditional well-defined databases. The new economy is more about analysing real-time flows of largely unstructured data: such as video streaming, images from social networks, data from IoT and sensor networks, high velocity event feeds from software defined infrastructure, and data provided by contributing parties in a global supply chain, to name a few.

All sorts of devices are becoming sources of data. The world is bristling with connected sensors, so that people and companies will leave a digital trail wherever they are, even if they are not connected to the internet.

EU Digital Single Market Strategy

The European Commission has recognised the importance of advancing the data economy, and has prioritised several actions in accordance with its Digital Single Market (**DSM**) strategy.

One such action is the General Data Protection Regulations (**GDPR**), which regulates the processing and use of **personal data** of EU citizens, regardless of where it sits. It represents a first fundamental milestone to creating a data-friendly environment where citizens and companies feel confident that their privacy preferences are protected, while also safeguarding economic interests and innovation.

The EU decided that regulation was needed as market forces alone cannot be relied upon to advance the data economy – essentially because of two main failures in the free data markets:

- a lack of transparency in data usage implied a risk of harm to business and citizens.
- market competition implied that data may not be shared optimally for the social good.

This whitepaper explores GDPR and related data regulations, and introduces VOLTA; an application developed by Guardtime to provide an intelligent solution to the new regulatory requirements, which leverages its KSI blockchain technology.

1 See www.guardtime.com

General Data Protection Regulations (GDPR)

In April 2016, the EU Parliament and Council agreed upon the General Data Protection Regulations[2] (**GDPR**), to go into effect on May 25, 2018. These regulations introduce tough new legal requirements and fines for companies relating to privacy and data protection of the **personal data** owned by EU individuals. They protect the citizens' rights enshrined in the EU Charter of Fundamental Rights (2009).

Essentially GDPR means it will soon be a legal requirement for companies to demonstrate **privacy by design, privacy by default** and lawful processing. GDPR is applicable to any organization—no matter where it resides—that handles the personal data of European Union residents or citizens. This is a big step up on the existing Data Protection Directive 95/46/EC requirements.

By strengthening data protection legislation and introducing tougher enforcement measures, the EU hopes to improve trust in the emerging digital economy.

> **"[GDPR]...With solid common standards for data protection, people can be sure they are in control of their personal information. And they can enjoy all the services and opportunities of a Digital Single Market."**
> Andrus Ansip, Vice-President for EU DSM

Governance of GDPR will be overseen by the National Data Protection Authorities (DPA).

In line with the DSM initiative, in January 2017 the EU also announced consistent proposals for regulations on Privacy and Electronic Communications (PECR) that will apply to all electronic communications.

It is instructive to look at the effects of the new regulation from the viewpoints of both the EU citizens, and the companies handling their personal data.

New Citizen Rights

GDPR defines key new EU citizen rights regarding the usage of their personal data by companies, which may be summarized as:

- **Informed** – Right to be informed of any personal data held, of how it is used or processed, of any breach, and of any disclosure/usage to third parties.
- **Consent** – Right to withdraw consent or restrict the processing or sharing of their data. Explicit and unambiguous informed consent must be obtained.
- **Access** – Right to secure direct access of own personal data, and to any processing, storage or sharing details.
- **Correct** – Right to rectify data if inaccurate or incomplete.
- **Forget** – Right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- **Portable** – A copy of the data held may be requested by the individual in a portable format.
- **Breach** – Right to be informed of any data breach that risks a person's rights and freedoms within 72 hours.

The EU definition of **personal data** is deliberately broad, meaning any data relating to an identifiable person. The link to the identity may be direct (name) or indirect (number, identifier, location, etc), and includes pseudonymized data.

The question that must be asked is how should institutions be reacting to these new regulations that are becoming enforceable soon?

2 Regulation EU 2016/679. see www.gdpr-info.eu

What Does GDPR Mean for Companies?

Even before these regulations came in, personal data had become an important and sensitive business commodity. However, GDPR marks a fundamental shift towards the view that privacy must be at the forefront of organizations' minds when dealing with "personal data".

GDPR requires companies that handle the personal data of EU citizens to undertake major operational reform so that they can demonstrate data privacy and protection by both design and default

It should be noted that GDPR comes with teeth. The Data Protection Authorities (**DPA**) may make announced and unannounced audits, and can administer fines up to 4% of global turnover or Euro 20mm.

> **"[GDPR]...the most significant change to European Union (EU) privacy law in decades"**
> Brendon Lynch, Microsoft's chief privacy officer

We would recommend that an organisation takes the following three steps:

1. Take a GDPR Risk Assessment

Review current practice against GDPR regulations – privacy risk. Key steps would include:

- Document the personal data (employee, customer, client, user, ...) the company holds, where it came from & when, who it is shared with, and how it stored and processed.
- Check the legal basis for and processing of personal data against GDPR i.e. procedures, consents and legal agreements in place.
- Determine whether the organisation is a data *'controller'* or *'processor'*, and whether it requires the appointment of a data protection officer (DPO).

2. Review Findings

GDPR defines new legal requirements that an organisation must be compliant with. Companies should review their findings against the key GDPR requirements to form a gap analysis including the following areas:

Accountability – compliance with the principles of GDPR including lawful processing of personal data.

Privacy by Design – that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle of the relevant data processing. Data security measures might involve data design, storage, transparency, monitoring, encryption, pseudonymisation, anonymization, & minimisation.

Privacy by Default – that, by default, only personal data which are necessary for each specific purpose of the processing should be collected and processed.

Rights of the Individual – that all the legislated new citizen rights are abided by ("Informed", "Consent", "Access", "Correct", "Forget", "Portable", "Breach").

Documentation – that an inventory of all personal data held, it's age, the processing and sharing activities, and related consents must be maintained. It must be available to the DPA or individual on demand

Breach Reporting – that the DPA and individual can be informed in a timely manner in the event of a data breach.

Impact Assessment – that a data protection impact assessment is undertaken as required to review the risk of harm through use or misuse of personal information.

3. Explore Solutions

Many companies will find their personal data storage practices and processing will need a major revamp in response to GDPR.

Guardtime's VOLTA product is an intelligent solution for GDPR for many companies, and is one of the first such product to be developed for this market. But first an introduction to Guardtime and its underlying KSI blockchain technology.

Guardtime and its KSI® Blockchain

Founded in 2007, Guardtime is understood to be the world's largest blockchain company by revenue, headcount and customers at the time of writing. It has the world's first massively scalable real-time authentication and integrity solution that handles any type of digital asset.

Guardtime invented KSI – a technology that allows any type of electronic activity to be independently verified using only formal mathematical methods, without the need for trusted insiders or cryptographic keys.

In production since 2009, this technology is proven, mature and battle-hardened. It provides the properties of **trust, integrity and provenance** required for the new data economies to flourish.

Guardtime's KSI technology is used across a variety of United States and European Union e-government and federal agency platforms to authenticate and validate important digital and M2M assets in real-time and regardless of scale; verifying their authenticity, time, chain-of-custody, interactions.

Estonia

Guardtime's KSI Blockchain is the fundamental integrity substrate for the Estonian e-Government systems[3] that have 1,000+ citizen e-services. Testing of KSI Blockchain in governmental systems started in 2008 and went live in 2012.

In many ways Estonia has led the EU down the Digital Single Market revolution, and it is positioned ahead of GDPR. Estonia already had individual consent enshrined in its Personal Data Protection Act (**PDPA**) of 2008. Citizens of Estonia trust that their data is held with integrity on the government systems because all access and data processing events are logged in the KSI blockchain.

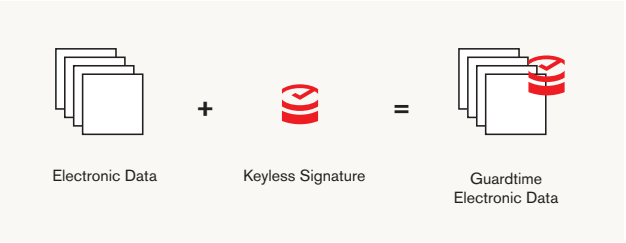
> **"[Estonia]...is the most advanced digital society in the world"**
> Wired

3 See www.e-estonia.com

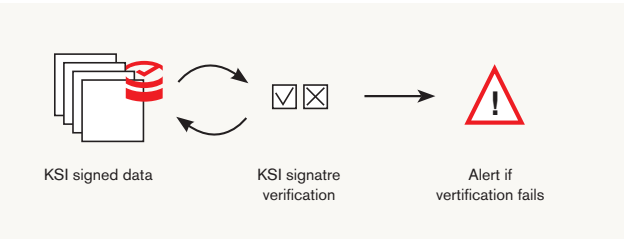
KSI® Blockchain

Guardtime's KSI blockchain is designed to provide massively scalable digital signature based authentication for electronic data, machines and humans.

Unlike traditional approaches that depend on asymmetric key cryptography, KSI uses only hash-function cryptography, allowing verification to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain.



Guardtime technology assigns a unique "keyless" signature to any type of data. The signature, is stored with the data, as an attribute which can be used to verify the time of creation, identity of creator and integrity of the data, independently from insiders, keys, secrets and certificates, and without the data leaving the premises.



Real time verification of the data signature occurs and notifications sent should data integrity be compromised and / or unauthorized access occur.

Guardtime has worked with partners to integrate its KSI technology seamlessly into their existing products including SAP cloud, Ericsson cloud, GE cloud and Oracle databases to name a few.

Additionally, Guardtime is working with partners to build solutions with its core KSI technology that are massively disruptive as befits the new data economy.

VOLTA: Assuring Governance of Personal Data for GDPR

VOLTA is a Guardtime solution for GDPR engineered to leverage over a decade of expertise in enabling immutable workflow, through the use of our KSI blockchain – often in the most demanding environments. VOLTA is designed to support the rigorous governance and compliance processes for managing personally identifiable information (**PII**), targeted by GDPR.

Today, personal data is held on many disparate systems and affects multiple *workflows* (i.e. applications, processes, and services). Integrating these disparate systems is a major challenge for tracking PII use. VOLTA takes a pragmatic approach to integration: firstly, by supporting light-touch interfaces such as CSV and REST, and secondly by enabling user-defined *policies* to be applied on all transactions associated with personal data handling.

At its simplest, VOLTA allows you to take 'snapshots' of transaction histories through simple CSV exports, using VOLTA Process Policy Maps (PPMs). Each workflow can have its own PPM, which defines the **schema, classification** of each field (personal, sensitive, classified etc.), and the **pseudonymisation** rules to apply. Alternatively, for tighter integration you can use a REST API to define ingestion rules.

Each workflow transaction is tracked according to its state, with the source, destination and context recorded. The level of granularity available depends on how much data is exposed to the system, and the pseudonymisation policies applied.

All PII related transactions are continuously registered in the KSI blockchain, providing an immutable history for auditors, tracking all transactions associated with each workflow.

Guardtime and its partners typically work with the client to ensure that all GDPR events associated with PII across the organization (i.e. consent, access, modification, copy etc.) are tracked in VOLTA and anchored in the KSI blockchain.

Where pseudonymisation is not required (if VOLTA is installed on site for example) then VOLTA essentially maintains a 'mirrored' signed copy of PII data, purely for audit purposes. Where pseudonymisation is enforced (e.g. where VOLTA is hosted remotely) then no PII data leaves the company network, and VOLTA maintains a signed copy of all key transactions using restricted identify information.

Today VOLTA is an intelligent solution for existing applications and services that require instrumenting for GDPR within an organization, all backed by the immutability and scale of the KSI blockchain. Workflows and processes can be instrumented with minimal integration issues, avoiding a major rewrite of existing infrastructure. Over time, deeper integration can be undertaken where appropriate to further strengthen immutability at core systems.

By leveraging industrial scale and low-latency transaction registration process of KSI, VOLTA runs in near real time, offering an automated immutable GDPR compliance service.

Guardtime's KSI blockchain provides the proof, provenance and trust required to satisfy compliance and audit requirements of GDPR and third parties such as regulators, auditors and the PII affected individuals.

Reporting

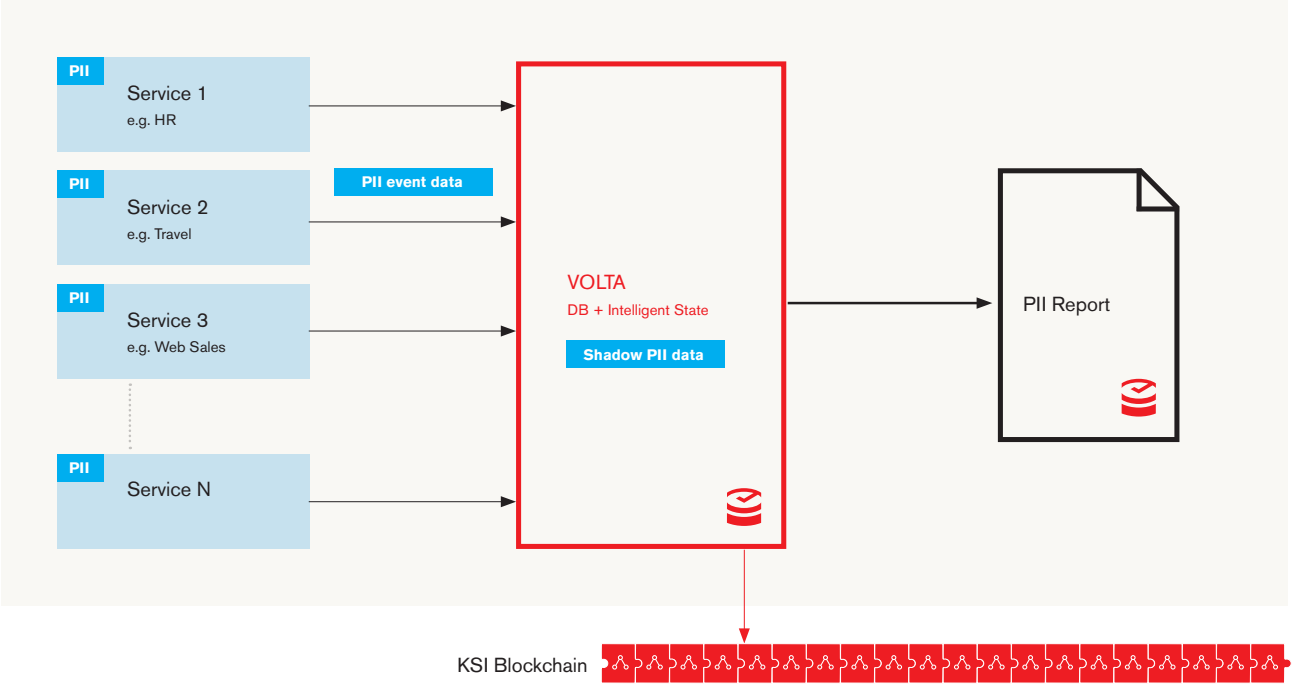
VOLTA offers role-based GDPR reports against the VOLTA database according to data handling policies, with data signed and verified by KSI. This offers independent verification to users, auditors and regulators that personal data is being handled appropriately.

In compliance with GDPR, VOLTA can produce high or low-level reports for the DPO, depending on the context, and the individual. This includes consent tracking and policy violation analytics. A REST API is available for partners and clients to create their own reports and analytics (again role based).

The VOLTA-DB contains all PII data events exposed to the system, signed and time-stamped, enabling correlation and frequency analysis on usage patterns (to flag misuse for example). With KSI verification running continuously in background, any data tampering can be notified and reported in near real-time.

Given the penalties associated with mishandling PII data under GDPR, VOLTA's functionality enables organizations to demonstrate governance in a pragmatic manner, bringing real business benefits and significantly de-risking the governance process.

Going forward we fully expect this platform to expand in the scope of both features and integration opportunities, to accommodate a broad set of compliance and workflow data instrumentation needs, backed by the surety of Guardtime's infrastructure and expertise in assuring data integrity, at scale.



Summary

In this whitepaper, we have briefly looked at the rapidly growing new data economy, and the response by government to bring in regulation such as GDPR to drive further growth.

The new GDPR regulations, financial penalties and mandatory breach disclosure requirements will raise the importance of the areas of data protection and privacy to being a key business consideration.

Guardtime created KSI blockchain technology to provide the missing properties of trust, integrity and provenance at massive scale. These are properties that stand-alone data does not have, especially if it has been sourced or processed in a separate environment out of direct sight or control. Estonia, the most advanced digital society in the world, has been using KSI blockchain for many years now as its e-government integrity layer.

In response to the GDPR regulations Guardtime has developed VOLTA; its intelligent solution for GDPR. VOLTA provides compliance with the auditing requirements of GDPR with the added benefits of trust, transparency and integrity that are inherent to a blockchain solution.

Guardtime's VOLTA product is an excellent solution to GDPR for many companies, especially for those companies whose personal data is spread across multiple systems and locations.

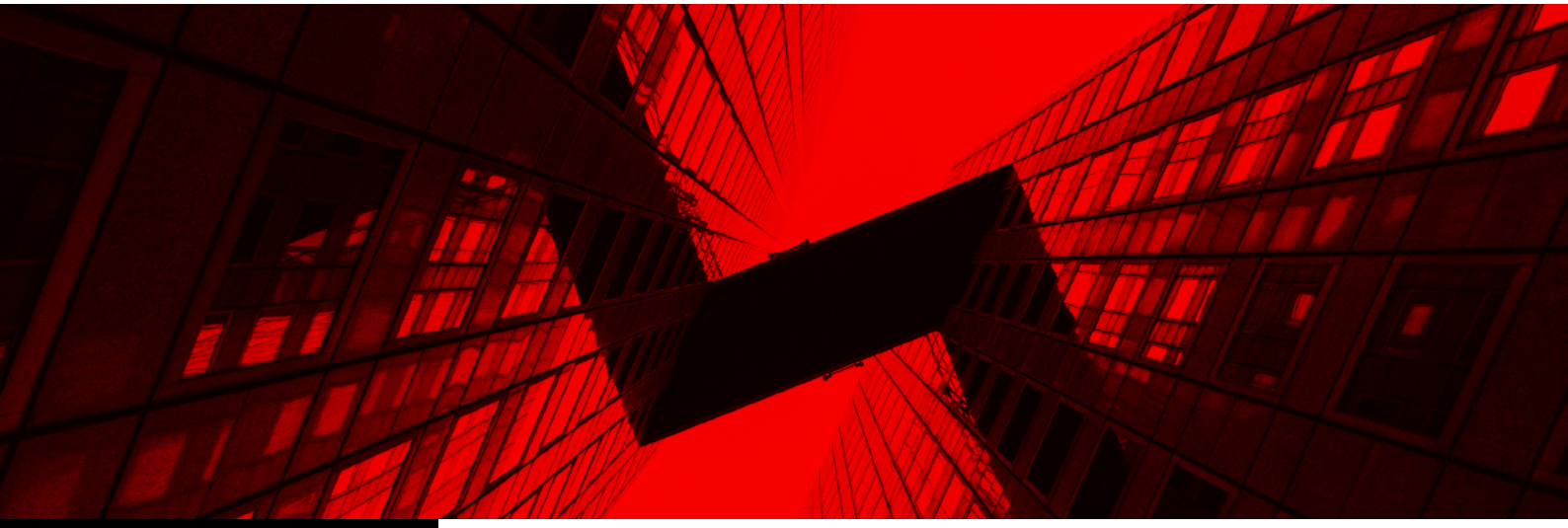
In addition to providing an immutable auditing service for GDPR, and a pathway to a GDPR compliant certification, VOLTA provides a continuous personal data compliance and over watch service, reducing the requirements for external audits, and providing the tools to flag bespoke data misuse and data tampering events for a company. These are tools that data savvy businesses should be incorporating to protect its data assets.

Furthermore, VOLTA is data agnostic like all KSI based technology, so its functionality may be extended to fulfil other compliance requirements that might exist for a company.

Finally, integration of KSI technology within an organisation opens the door to the incorporation of other new data economy solutions that will drive efficiency and profits. One such example is the management of the physical, information and software supply chains that exist starting from suppliers, and running all the way to end customers/consumers.

Please get in contact if you would like to know more about VOLTA, our pragmatic solution for GDPR, or to discuss your findings and requirements following an internal GDPR risk assessment.

David Shorthouse
Product Manager for Compliance and GDPR
david.shorthouse@guardtime.com



guardtime

info@guardtime.com
guardtime.com

Photos: Heidi Sandstrom, Samuel Zeller